AF
ZJW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Gerald R. Malan et al.

Group Art Unit: 2142

Examiner: Benjamin Ailes

Serial No.: 09/855,810

Filed: May 15, 2001

For: METHOD AND SYSTEM FOR RECONSTRUCTING A PATH TAKEN BY UNDESIRABLE NETWORK TRAFFIC

Attorney Docket No.: UOM 0208 PUSP

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop Appeal Brief - Patents
Commissioner for Patents
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an Appeal Brief from the final rejection of claims 1-20 of the Office Action mailed on April 21, 2005 for the above-identified patent application.

I. REAL PARTY IN INTEREST

The real party in interest is The Regents of the University of Michigan ("Assignee"), a non-profit corporation organized and existing under the laws of the state of Michigan, and having a place of business at 3003 S. State Street, Ann Arbor, MI 48109, as

CERTIFICATE OF MAILING UNDER 37 C.F.R. § 1.8

I hereby certify that this paper, including all enclosures referred to herein, is being deposited with the United States Postal Service as first-class mail, postage pre-paid, in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, U.S. Patent & Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 on:

9-15-05 — **Date of Deposit**

David R. Syrowik — **Name of Person Signing**

Signature

set forth in the assignment recorded in the U.S. Patent and Trademark Office on May 15, 2001 at Reel 011813/Frame 0370.

II. RELATED APPEALS AND INTERFERENCES

There is a related appeal in application Serial No. 09/855,808 for "method and System for Detecting, Tracking and Blocking Denial of Service Attacks Over a Computer Network," which may directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-20 are pending in this application. Claims 1-20 have been rejected and are the subject of this appeal.

IV. STATUS OF AMENDMENTS

A Reply after final rejection was filed on June 15, 2005. No Amendments have been denied entry.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The claimed subject matter is a method and system for reconstructing a path taken by undesirable network traffic through a computer network from a source of the traffic, as indicated by the following: a) the title of the application; b) the first sentence of the abstract; c) the field of the invention; d) the object of the invention; and e) independent claims 1 (*i.e.*, method) and 9 (*i.e.*, system).

The method initially includes the step of collecting statistics at a plurality of measurement points located within routing and forwarding infrastructure of the computer network. The method and system are described in detail on page 16, line 26 through page 18, line 32 of the application under the heading "Storm Tracker and Storm Breaker." As described therein, "Storm Tracker" uses statistics gathered directly from the Internet routing and forwarding infrastructure to back trace Internet denial service attacks. Packet and flow statistics are gathered directly from the Internet routing and forwarding infrastructure (also called forwarding infrastructure). By collecting flow statistics directly from the forwarding infrastructure, the tracker is able to trace attacks that are untraceable by the prior art. Figure 6 shows an example of denial of service attack that can be tracked through a sample network. The path of the attack traffic goes from the attacker, through Router A, through Router B, and then through Router C to the target.

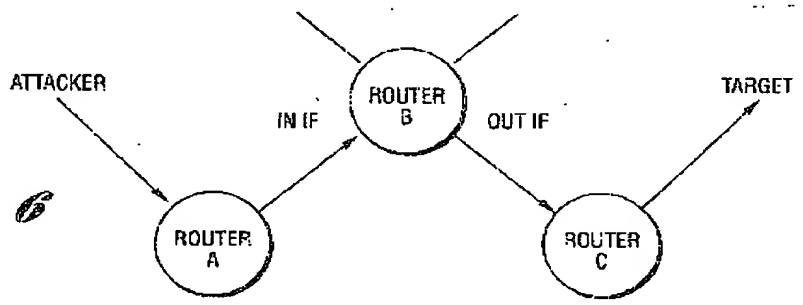

Fig. 6

Again, one of the key features of the claimed invention is that the statistics are taken directly from the forwarding infrastructure itself to determine the path of the attack traffic.

Figure 7 illustrates the trackers overall architecture.

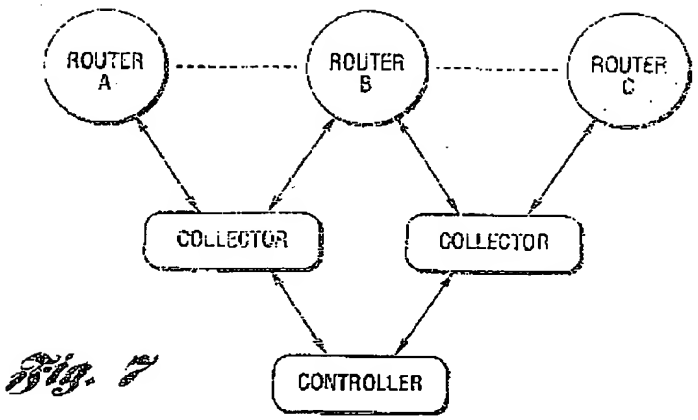

Fig. 7

Figure 7 shows two stages of the architecture: collectors and a controller. The collectors interface with the forwarding infrastructure in that they collect the statistics and report the findings to the controller. The tracker's collectors take samples of the statistics from the forwarding infrastructure. Typically, two types of statistics that routers may collect include single packet statistics and flow-based statistics. Single packet statistics are those that provide important information about a set of packets entering a forwarding node, *i.e.*, a router. Some of the statistics kept include: destination and source IP address, incoming interface, protocol, ports, and length.

Flow-based statistics are statistics that describe a set of packets that are related to the same logical traffic flow. The concept of flow is generally defined as a stream of packets that all have the same characteristics: source address, destination address, protocol type, source port, and destination port. Such statistics may either be directional or bidirectional. Flow statistics aggregate a flow's individual packet statistics into a single statistic. Examples include a flow's duration, number of packets, mean bytes per packet, etc.

The statistics are analyzed by the controller to reconstruct the path taken by the undesirable network traffic through the network from the source of the traffic. Once a

controller has received the statistics from the collectors, it takes one of two approaches to trace the attacks: 1) directed tracing; and 2) distribution correlation. In directed tracing, one utilizes the knowledge of network topology to work backward toward the source of the attack. With the distributed correlation, the controller compares the attack signature with those discovered at other nodes in the topology. Attacks which correlate strongly are associated together and implicitly form a path from the source to the target.

Directed tracing relies on the fact that one has both the router's incoming interface statistics for an attack and the knowledge of the topology to determine what routers are upstream on that link. With this knowledge, upstream routers can then be queried for their participation in transiting the attack. Since the upstream routers are looking for a specific attack signature, it is much easier to find the statistics of merit.

In the distribution correlation approach, a general attack profile is extracted from every router's statistics to uncover the global path for the attack.

In summary, the statistics are analyzed to reconstruct the path taken by the undesirable network traffic through the network from the source of the traffic.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-3, 6, 8-11, 14 and 16-20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the U.S. patent to Soha, 4,817,080 in view of the published article by Smith et al. entitled "Operating Firewalls Outside the LAN Perimeter."

Claims 4, 5, 7, 12, 13 and 15 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the U.S. patent to Soha in view of the article by Smith et al., and further in view of the U.S. patent in the name of Phaal, 5,315,580.

VII. ARGUMENT

A. Claims 1-3, 6, 8-11, 14 and 16-20 are Patentable Under 35 U.S.C. § 103(a) Over U.S. Patent No. 4,817,080 (Soha) in View of the Publication of Smith et al.

The U.S. Patent to Soha which is cited on page 3, lines 13-15 of the application discloses a system that measures traffic statistics by looking at packet contents. Soha is concerned with monitoring a statistics-bearing communication bus (or legs of a local area network) to guarantee that complete statistics are collected. The system collects distributed measurements and forwards them to a centralized point.

Soha is not concerned with collecting statistics at a plurality of measurement points in routing and forwarding infrastructure in order to reconstruct a path taken by undesirable network traffic through a computer network from a source of the traffic as only provided by the present invention.

Smith, et al. is concerned with placing fire walls outside corporate network boundaries, into the Internet, to block an attacker. Clearly, Smith, et al. is not concerned with analyzing statistics in order to reconstruct a path taken by undesirable network traffic through a computer network from a source of the traffic. While Smith, et al. discusses multiple paths from a source of an attack there is no discussion of reconstructing such a path or paths.

Contrary to the Examiner's position, "reconstruction of the path" from a source of the undesirable network traffic is not the same as a method used to block or control traffic from getting to its destination. In other words, "blocking" is not the same as "reconstructing." Rather, "reconstructing" means to "rebuild" or "put together again" or "reassemble." Dependent claims 2 and 10 call for the additional step of "blocking" in addition to the step of "reconstructing" in the present application. Hence, again "blocking" is not the same as "reconstructing."

Furthermore, the Examiner has not pointed to any teaching within either of the cited references to suggest the proposed combination of references. Soha is simply not concerned with collecting statistics in order to deal with undesirable network traffic. Consequently, one of ordinary skill in the art would not look to Soha to solve the problem only addressed by the present invention. However, even if the combination could be made, the combination would not result in the claimed invention.

In summary, the method of "blocking" in Smith, et al. is not the same as "reconstructing" a path taken by undesirable network traffic through a computer network from a source of the traffic as only provided by the present invention.

The fee of $250.00 as applicable under the provisions of 37 C.F.R. § 41.20(b)(2) is enclosed. Please charge any additional fee or credit any overpayment in connection with this filing to our Deposit Account No. 02-3978.

Respectfully submitted,

Gerald R. Malan et al.

By: _____
David R. Syrowik
Registration No. 27,956
Attorney for Applicants

Date: 9-15-05

BROOKS KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075-1238
Phone: 248-358-4400
Fax: 248-358-3351

Enclosure - Appendices

VIII. CLAIMS APPENDIX

1. A method for reconstructing a path taken by undesirable network traffic through a computer network from a source of the traffic, the method comprising:

collecting statistics at a plurality of measurement points located within routing and forwarding infrastructure of the computer network; and

analyzing the statistics to reconstruct the path taken by the undesirable network traffic through the network from the source of the traffic.

2. The method as claimed in claim 1 further comprising blocking undesirable network traffic within the computer network upstream of the points based on the reconstructed path.

3. The method as claimed in claim 1 wherein the routing and forwarding infrastructure includes at least one router.

4. The method as claimed in claim 1 wherein the statistics include flow-based statistics which provide information related to the same logical traffic flow.

5. The method as claimed in claim 1 wherein the statistics include packet statistics which provide information about a set of packets entering the routing and forwarding infrastructure.

6. The method as claimed in claim 1 further comprising requesting and receiving upstream statistics from forwarding infrastructure of the computer network upstream the measurement points and wherein the step of analyzing includes the step of analyzing the upstream statistics to reconstruct the path taken by the undesirable network traffic.

7. The method as claimed in claim 1 wherein the step of analyzing includes the step of extracting profiles from the statistics collected at the plurality of measurement points and comparing the profiles to reconstruct the path taken by the undesirable network traffic.

8. The method as claimed in claim 1 wherein the computer network is the Internet.

9. A system for reconstructing a path taken by undesirable network traffic through a computer network from a source of the traffic, the system comprising:

collectors for collecting statistics at a plurality of measurement points located within routing and forwarding infrastructure of the computer network; and

at least one controller in communication with the collectors for analyzing the statistics to reconstruct the path taken by the undesirable network traffic through the network from the source of the traffic.

10. The system as claimed in claim 9 further comprising means in communication with the at least one controller for blocking undesirable network traffic within the computer network upstream of the points based on the reconstructed path.

11. The system as claimed in claim 9 wherein the routing and forwarding infrastructure includes at least one router.

12. The system as claimed in claim 9 wherein the statistics include flow-based statistics which provide information related to the same logical traffic flow.

13. The system as claimed in claim 9 wherein the statistics include packet statistics which provide information about a set of packets entering the routing and forwarding infrastructure.

14. The system as claimed in claim 9 further comprising means for requesting and receiving upstream statistics from forwarding infrastructure of the computer network upstream the measurement points and wherein the at least one controller analyzes the upstream statistics to reconstruct the path taken by the undesirable network traffic.

15. The system as claimed in claim 9 wherein the controller extracts profiles from the statistics collected at the plurality of measurement points and compares the profiles to reconstruct the path taken by the undesirable network traffic.

16. The system as claimed in claim 9 wherein the computer network is the Internet.

17. The method as claimed in claim 1 wherein the undesirable network traffic includes denial of service attacks.

18. The method as claimed in claim 17 wherein the computer network includes a plurality of service provider networks.

19. The system as claimed in claim 9 wherein the undesirable network traffic includes denial of service attacks.

20. The system as claimed in claim 19 wherein the computer network includes a plurality of service provider networks.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.